UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/767,980	01/29/2004	James William Fahrny	CCCI 0128 PUS	5334

50764 7590 04/04/2008

BROOKS KUSHMAN P.C.
1000 TOWN CENTER
TWENTY-SECOND FLOOR
SOUTHFIELD, MI 48075

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
04/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/767,980
Filing Date: January 29, 2004
Appellant(s): FAHRNY ET AL.

James N. Kallis
Reg. No. 41,102
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed January 4, 2008 appealing from the Office action mailed August 2, 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is incorrect. A correct statement of the status of the claims is as follows:

This appeal involves claims 1-3, 5-13, 15-21, and 23-28.

Claims 4, 14, and 22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is incorrect. The amendment after final rejection filed on September 26, 2007 has been entered.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner: dependent claims 4, 14, and 22 have since been found to be allowable over the previously cited references, in view of Appellant's arguments presented in the Appeal Brief.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,424,717	PINDER	7-2002
5,784,095	ROBBINS	7-1998

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-3, 5, 6, 8, 9, 11-13, 15, 16, 19-21, 23, 24, and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pinder (U.S. Patent 6,424,717) in view of Robbins (U.S. Patent 5,784,095).

Regarding claims 1 and 11:

Pinder discloses a method and system for multi-stream security processing and distributing digital media streams comprising: a head-end configured to generate

encrypted digital media streams (element 515 of Figure 5); a network coupled to the head-end and configured to receive the encrypted digital media streams (elements 517/523 of Figure 5); and at least one receiver coupled to the network and configured to receive the encrypted digital media streams and present a decrypted version of the encrypted media streams, wherein at least one of the head-end and the at least one receiver comprise a security processor configured to provide at least one of the simultaneous multiple encryption and decryption processing of the streams (col. 4, lines 30-50). Although Pinder discloses being able to configure, renew, and reconfigure at least one of the encryption and decryption processes by the security processor through the use of downloaded updates (col. 25, lines 28-50; col. 26, lines 54-63; col. 29, etc.), it does not explicitly state that such updates comprise downloaded software/firmware. However, the ability of set-top boxes and related devices capable of processing digital media streams to download firmware updates and store them in memory has long since been known to be obvious in the art; one such example is disclosed by Robbins (col. 5, lines 1-6; col. 13, lines 65-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made for a set-top box in accordance with the Pinder invention to download firmware updates to modify the device's functionality. The motivation for doing so would be to easily accommodate new features or changes in requirements, including for security (Robbins, Ibid).

Regarding claim 20:

Pinder discloses a security processor comprising a controller (col. 10, lines 55-65), a memory for storing downloaded updates (col. 22, lines 1-45) and a plurality of digital stream encryption/decryption engines that are selectively parallel coupled by the controller for simultaneous operation in response to a predetermined security configuration (elements 234, 236, and 238 of Figure 2B; col. 7, lines 1-15).

Although Pinder discloses wherein the controller is operative to be programmed through download from a head-end, each download operative to modify media stream processing by the security processor (col. 25, lines 28-50; col. 26, lines 54-63; col. 29, etc), it does not explicitly disclose wherein the downloads comprise firmware. However, the ability of set-top boxes and related devices capable of processing digital media streams to download firmware updates and store them in memory has long since been known to be obvious in the art; one such example is disclosed by Robbins (col. 5, lines 1-6; col. 13, lines 65-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made for a set-top box in accordance with the Pinder invention to download firmware updates to modify the device's functionality. The motivation for doing so would be to easily accommodate new features or changes in requirements, including for security (Robbins, Ibid).

Regarding claims 2, 12, and 21:

Pinder further discloses wherein the media streams are at least one of a video stream, audio stream, or video plus audio stream (e.g. col. 6, lines 15-20; Fig. 7).

Regarding claims 3 and 13:

Pinder further discloses wherein the security processor further comprises a plurality of digital stream encryption/decryption engines that are selectively [parallel] coupled by the controller for simultaneous operation in response to a predetermined security configuration (elements 234, 236, and 238 of Figure 2B; col. 7, lines 1-15).

Regarding claims 5, 15, and 23:

Pinder further discloses wherein the security configuration management comprises at least one of a secure download, RSA key management, multiple security key management, authentication, copy protection, and digital signatures (e.g. col. 6, lines 50-65).

Regarding claims 6, 16, and 24:

Pinder further discloses wherein the security processor further comprises at least one of a memory containing a hash, engine encryption/decryption configuration logic, a random number generator, a multiplier, and a memory containing a dynamic feedback arrangement scrambling technique (DFAST) algorithm coupled [in parallel] to the controller and configured to provide multiple key management for at least one of conditional access and digital rights management (e.g. col. 6, lines 25-30).

Regarding claims 8, 19, and 27:

Pinder further discloses wherein the security processor provides a role-based authentication that is used by an authorized user for at least one of configuration, reconfiguration, and renewal (col. 10, lines 5-25).

Regarding claims 9 and 28:

Pinder further discloses wherein the receiver is at least one of a set-top box (STB), and a receiver or transceiver for at least one of digital television, HDTV, audio, MP3, text messaging, and game digital streams (col. 7, lines 25-32).

Regarding claim 26:

Pinder further discloses wherein the system for multistream security processing and distributing digital media streams comprises a headend (element 515 of Figure 5), a network electrically coupled to the headend, a set-top box (STB) coupled to the network (elements 517/523 of Figure 5), and a receiver coupled to the STB, and the security processor is implemented in connection with at least one of the headend, the network, the STB, and the receiver (col. 4, lines 30-50).

Claims 7, 17, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pinder in view of Robbins as applied to claims 1, 11, and 20 above, and further in view of the "POD Copy Protection System" (hereinafter, "Cablecard").

Regarding claims 7, 17, and 25:

Although Pinder discloses both RAM and flash memory containing the predetermined security secrets (col. 47, lines 10-15), neither it nor Robbins explicitly recites wherein the memory is swappable. However, Cablecard discloses a system wherein the security secrets can be stored on the memory of a swappable component (page 7, "Historical Perspective"; secrets at Table 4.2-A for example). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the security functions of the set-top box on a swappable memory card. The motivation for doing so would be to allow for unscrambling of digital cable streams (Cablecard, page 1, "1.1 Scope", 1st paragraph). It is additionally noted that making this change would allow one to remain in compliance with U.S. laws and regulations in effect at the time the invention was made (see the enclosed FCC reference).

Claims 10 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pinder in view of Robbins as applied to claims 1 and 11 above, and further in view of "HDCP: what it is and how to use it" (hereinafter, "HDCP").

Regarding claim 10:

Pinder discloses a set-top box receiver (col. 4, lines 30-50) and an additional receiving device including the security processor (the "intelligent" television, col. 7, lines 28-35), which can be configured to receive and decrypt encrypted digital media streams using the security processor. However, neither Pinder nor Robbins appears to disclose

wherein the STB and intelligent television are coupled to each other, allowing for encrypted communication between those two devices. Regardless, HDCP discloses that a set-top box and a television can be coupled to each other, each containing a security processor that encrypts and decrypts content over the link between those devices (HDCP, page 1, "System Architecture"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to couple an STB and television in such a way as to allow the STB to transmit encrypted media streams to the television. The motivation for doing so would be to protect copyrighted media without infringing on customer-demanded features (page 1, "What HDCP is—and isn't").

Regarding claim 18:

Although Pinder discloses coupling an additional receiving device to the receiver (col. 4, lines 30-35), neither Pinder nor Robbins appear to disclose presenting the encrypted digital media streams from the receiver to the additional receiving device, whereupon the streams are decrypted using the additional receiving device's security processor. However, HDCP discloses that a set-top box and a television can be coupled to each other, each containing a security processor that encrypts and decrypts content over the link between those devices (HDCP, page 1, "System Architecture"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to couple an STB and television in such a way as to allow the STB to transmit encrypted media streams to the television. The motivation for doing so would be to

protect copyrighted media without infringing on customer-demanded features (page 1, "What HDCP is—and isn't", particularly the first two paragraphs).

(10) Response to Argument

Examiner believes that Appellant's arguments are in error, based upon Appellant's narrow interpretation of the disputed claim language. Beginning with claims 1 and 11, the following limitations most pertinent to the arguments made by Appellant are reprinted herein:

> Claim 1: "...the security processor operative to store the downloaded software and to securely configure, renew, and re-configure at least one of encryption and decryption by the security processor based on the downloaded software."
> Claim 11: "...reconfiguring a security processor in the received based on the software download to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams; ..."

From Appellant's remarks it is fairly clear that Appellant has interpreted these limitations to be narrowly limited to wherein the software update alters the actual algorithm - the software code - that the device uses to perform encryption or decryption; this is best illustrated by Appellant's arguments on beginning on page 8, last paragraph, through page 9, 1st paragraph, and also page 10, wherein Appellant declares "The decryption is accomplished by the downloaded software". Examiner strongly disagrees, maintaining that the actual claim language is significantly broader in scope than Appellant's preferred interpretation, and while that interpretation is clearly supported by

the instant specification, it is emphatically **not** what is recited by the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Instead, what is claimed is merely the ability to reconfigure the device's ability to perform either encryption or decryption *in some unspecified fashion*, which could also be accomplished merely by reconfiguring the keys used by a pre-existing encryption/decryption algorithm. For example, it is observed that Pinder discloses the use of Entitlement Control Messages (ECMs) and Entitlement Management Messages (EMMs) to distribute keys to configure, renew, and re-configure the device to determine which media streams a subscriber is entitled to watch (see column 4 of Pinder for example). Of particular interest is the following passage:

> As shown in detail with regard to set top box 113(0), set top box 113 includes decryptor 115, which uses a control word 117 as a key to decrypt encrypted instance 105. Control word 117 is produced by control word generator 119 from information contained in entitlement control message 107 and information from authorization information 121 stored in set-top box 113. For example, authorization information 121 may include a key for the service and an indication of what programs in the service the subscriber is entitled to watch. If the authorization information 121 indicates that the subscriber is entitled to watch the program of encrypted instance 105, control word generator 119 uses the key together with information from ECM 107 to generate control word 117. Of course, a new control word is generated for each new ECM 107. [Pinder, col. 4, lines 37-51]

This passage rather clearly recites that the keys used for decryption by the content are determined by which channels a user is subscribed to. Thus, since the keys used materially affect the decryption process, Appellant's arguments to the contrary (pages 8-9 of the Appeal Brief, Ibid) are demonstrably in error.

The sole reason why the Pinder reference was determined not to anticipate each limitation of the claims lay in the fact that while the keys that the Pinder set-top box uses are distributed in ECMs and/or EMMs, these are not "software" *per se* but rather data structures that would be acted upon by software already resident in the Pinder device. All that would remain for the prior art to show is a suggestion that this information could be included as part of a software download to the set-top box; this is precisely what Robbins discloses at col. 13, line 65 – col 14, line 1: "The separate control channel updates the system firmware[1] stored in ROM 337 with new releases **whenever user subscriptions change or for security**." (emphasis Examiner's). As is clearly seen in Pinder, a change in subscription necessarily entails a change in the keys used by the set-top box to decrypt various channels, which in turn constitutes a reconfiguring of the decryption or encryption by the security processor based on the software update. It is also observed that in addition to the motivation expressly recited by the Examiner in Final Office Action of 8/2/07, it should also be readily apparent from at least the Robbins disclosure that the technique of a set-top cable box downloading a firmware update has clearly been well known among those of ordinary skill in the art as a means to supply updated configuration information to such a device, and such an improvement would yield predictable results: *KSR v. Teleflex*, 550 U.S. at ___, 82 USPQ2d at 1395-1397.

Appellant's remaining arguments traversing the rejections of claims 1 and 11 (through page 11 of the Appeal Brief) are similarly predicated on the narrow interpretation that the software download must necessarily comprise the actual code

[1] "Firmware" being a software program controlling the microprocessor: Robbins, col. 4, lines 65-67.

used to perform encryption and/or decryption, and are thus addressed by Examiner's remarks above. For at least these reasons, Examiner respectfully requests that the rejections of claims 1 and 11 be upheld.

Claim 20 recites an alternate embodiment of the invention of claims 1 and 11, wherein Appellant argues that the prior art fails to disclose the following limitation regarding "a controller operative to be programmed through authenticated firmware downloads from a headend, each firmware download operative to modify media stream processing by the security processor" (see the Appeal Brief, page 13, 1st original paragraph). It is observed that this limitation is even broader than what is found in claims 1 and 11, in that claim 20 does not even recite wherein the firmware download is required to alter decryption or encryption in any way, but instead discloses that it can make *any* modification that could alter the device's ability to process media streams. Examiner maintains that sending new encryption keys to a cable box easily reads upon at least the broadest reasonable interpretation of the disputed claim language. As established in the Final Office Action, Pinder discloses authenticated downloads (via EMM/ECM data structures: e.g. col. 4 as cited above) to modify that device's ability to process media streams; while Robbins establishes that such updates can be bundled as part of a firmware update (col. 13, lines 65-67). Thus, Examiner's arguments presented *supra* regarding claims 1 and 11 are equally applicable to claim 20; accordingly, for at least all the reasons set forth above, Examiner respectfully requests that the rejection of claim 20 be upheld.

With respect to claim 22, upon consideration of Appellant's arguments Examiner now concedes that this claim, by merit of the fact that it explicitly recites wherein the downloaded update includes executable software code intended for execution on the device for at least one of the DES, Triple-DES, AES, or CSA encryption algorithms, the claim would be allowable over the cited prior art rejections. Additionally, though not explicitly argued by the Appellant, claims 4 and 14 disclose similar limitations and would also be allowable over the previously cited prior art.

With respect to claim 23, again the Appellant presumes the narrow interpretation that the firmware update must necessarily comprise the software to perform encryption and/or decryption. As has been repeatedly established *supra*, this is clearly not the case. Thus, Examiner respectfully requests that the rejection of claim 23 be upheld for at least substantially similar reasons as discussed in the rejection of claim 20 above.

Examiner also respectfully requests that the rejections of all remaining dependent claims not previously addressed above also be upheld for substantially similar reasons as discussed *supra*.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,
/Thomas Gyorfi/
Examiner, Art Unit 2135
Thomas Gyorfi

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Conferees:

/G. B./
Supervisory Patent Examiner, Art Unit 2132

/Christian LaForgia/
Primary Examiner
Art Unit 2139